

1/3/4

DIALOG(R)File 351:Derwent WPI

(c) 2003 Thomson Derwent. All rts. reserv.

009551044 \*\*Image available\*\*

WPI Acc No: 1993-244591/199331

Related WPI Acc No: 1995-081028; 1995-100487

XRPX Acc No: N93-188078

Switched telecommunications network security system - uses network security node to transform information between subscribing parties from encrypted to decrypted form or vice versa as required  
Patent Assignee: AMERICAN TELEPHONE & TELEGRAPH CO (AMTT ); AT & T CORP (AMTT )

Inventor: BULFER A F; KAPLAN M M; MCNAIR B E; WEGRZYNOWICZ C A

Number of Countries: 008 Number of Patents: 005

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 553553	A2	19930804	EP 92311093	A	19921204	199331 B
CA 2080929	A	19930610	CA 2080929	A	19921020	199335
JP 6085811	A	19940325	JP 92351390	A	19921208	199417
US 5392357	A	19950221	US 91803809	A	19911209	199513
EP 553553	A3	19941123				199536

Priority Applications (No Type Date): US 91803809 A 19911209

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
-----------	------	-----	----	----------	--------------

EP 553553	A2	E	24	H04Q-003/58	
-----------	----	---	----	-------------	--

Designated States (Regional): DE ES FR GB IT

JP 6085811	A		23	H04L-009/00	
------------	---	--	----	-------------	--

US 5392357	A		22	H04M-001/68	
------------	---	--	----	-------------	--

CA 2080929	A			H04L-009/28	
------------	---	--	--	-------------	--

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-085811

**(43)Date of publication of application : 25.03.1994**

(51)Int.Cl.

H04L 9/00  
H04L 9/10  
H04L 9/12  
H04L 12/00  
H04Q 3/545

(21)Application number : 04-351390

(71)Applicant : AMERICAN TELEPH & TELEGR CO <ATT>

(22)Date of filing : 08.12.1992

(72)Inventor: BULFER ANDREW F  
KAPLAN MICHAEL M  
MCNAIR BRUCE E  
WGRZYNOWICZ CAROL A

(30)Priority

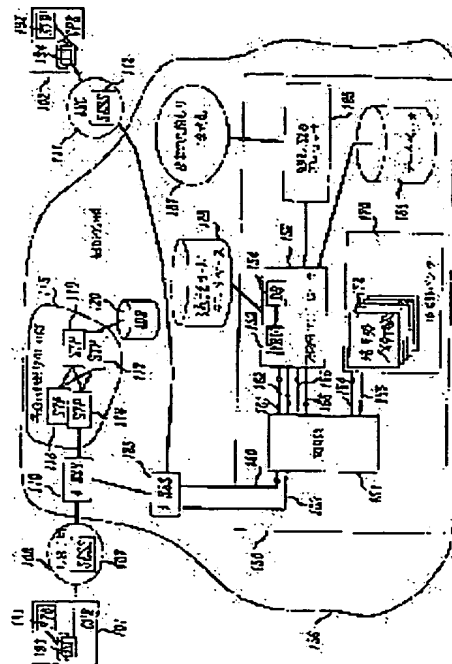
Priority number : 91 803809      Priority date : 09.12.1991      Priority country : US

(54) METHOD AND SYSTEM FOR MAKING COMMUNICATION VIA EXCHANGE NETWORK AVAILABLE, METHOD FOR PROVIDING SECURITY FUNCTION TO SECURITY NODE AND EXCHANGE NETWORK, METHOD FOR PROCESSING ENCRYPTED COMMUNICATION, AND METHOD FOR PROVIDING SECURITY COMMUNICATION

**(57)Abstract:**

**PURPOSE:** To provide comparatively secure communication even when parties concerned of a call use a security device with different protocols and algorithms by placing a security node that explains a security signal received from a CPE before information is delivered to a called party in a non-encryption form.

**CONSTITUTION:** A security node 150 placed to an electric communication network connecting a caller and a called party has a converter 151, a controller 152 converts received encrypted voice and data signals into information or non-encryption information encrypted by a different form in cooperation with the exchange 151 and conducts the inverse conversion. The controller 152 gives a control signal relating to the type of selected encryption used by the caller to the exchange 151. In the case of calling a hunt group, a proper encryption device such as 172 is selected and the controller 152 is used for the processing. The call signal is fed from the controller 152 to the exchange 151 through a conductor wire 168, and reverse communication, that is, communication from the called party 102 to the caller 101 takes the same path when the call path is once formed by the exchange 151 and an encryption device 172 in the return direction is used.



## LEGAL STATUS

[Date of request for examination] 25.05.1993

[Date of sending the examiner's decision of rejection] 02.04.1996

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号

特開平6-85811

(43)公開日 平成6年(1994)3月25日

(51)Int.Cl.<sup>5</sup>

識別記号

庁内整理番号

FI

技術表示箇所

H04L 9/00  
9/10  
9/12

7117-5K  
8529-5K

H04L 9/00  
11/00

Z

審査請求 有 請求項の数25(全 23 頁) 最終頁に続く

(21)出願番号 特願平4-351390

(22)出願日 平成4年(1992)12月8日

(31)優先権主張番号 803809

(32)優先日 1991年12月9日

(33)優先権主張国 米国(US)

(71)出願人 390035493

アメリカン テレフォン アンド テレグ  
ラフ カムパニー

AMERICAN TELEPHONE  
AND TELEGRAPH COMPA  
NY

アメリカ合衆国 10013-2412 ニューヨ  
ーク ニューヨーク アヴェニュー オブ  
ジ アメリカズ 32

(74)代理人 弁理士 三俣 弘文

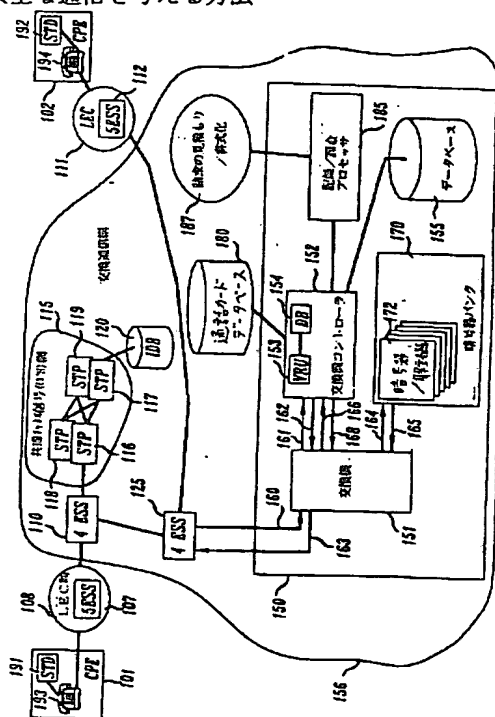
最終頁に続く

(54)【発明の名称】 交換網を介する通信を可能とする方法およびシステム、安全ノード、交換網に安全機能を与える方法、暗号化通信を処理する方法、ならびに安全な通信を与える方法

(57)【要約】

【目的】 呼の両当事者がプロトコルおよびアルゴリズムの異なる安全装置を用いたり、安全装置を一方しか持たない場合も、比較的安全な通信を与える。

【構成】 発呼者と被呼者を接続する電気通信網に配置された安全ノードが、第1の形式で暗号化された情報(音声、データ等)を(a)異なる形式で暗号化された情報または(b)非暗号化情報に変換し、またこの逆変換も行う。安全ノードは通信網に接続された任意の場所からアクセスできる。呼またはメッセージに安全ノード経由の経路を与え、安全ノードに適切な制御信号を与えることにより、当事者間の伝送経路の部分のみにおいて情報を暗号化し、他の部分は情報をクリア(暗号化しない)とすることができる。または、異なる暗号アルゴリズムを用いて、経路の異なる部分で情報を暗号化することもできる。



## 1

## 【特許請求の範囲】

【請求項1】 交換通信網を含む呼経路を介して発呼者と被呼者との間の通信を可能とするために、前記発呼者によって発信され前記被呼者に宛てられ且つ暗号化情報を前記通信網に適用するCPE（加入者構内装置）と、前記交換網に配置されていて、前記CPEから受信した前記の暗号化情報を該情報が前記被呼者に非暗号化形式で伝達される前に解読するように構成された安全ノードとを備え、前記呼経路の少なくとも一部分にわたる通信が暗号化され、かつ前記呼経路の残りの部分にわたる通信がクリア（非暗号化）であることを特徴とする交換網を介する通信を可能とするシステム。

【請求項2】 前記安全ノードが、交換機と、複数の暗号解読器と、前記の暗号化情報に前記暗号解読器のうちの特定の解読器への経路を設定するために前記交換機を制御する制御手段とを備えたことを特徴とする請求項1記載のシステム。

【請求項3】 前記制御手段が、データベースと、前記CPEにおいて使用される暗号の型を判定する手段と、前記暗号型の各々を前記暗号解読器のうちの特定の解読器に関係付けて前記データベースに記憶されている情報を検索する手段とを備えたことを特徴とする請求項2記載のシステム。

【請求項4】 発呼者から暗号化情報を受信する手段と、前記の暗号化情報に、対応する非暗号化情報を生成するための解読器を通して経路を与える手段と、前記の非暗号化情報を前記被呼者に送る手段とを備えた交換通信網に配置されることを特徴とする安全ノード。

【請求項5】 交換通信網を含む呼経路を介して発呼者と被呼者との間の通信を可能とするために、前記発呼者によって発信され前記被呼者に宛てられ且つ非暗号化情報を前記通信網に適用するCPE（加入者構内装置）と、前記交換網に配置されていて、前記CPEから受信した前記の非暗号化情報を該情報が前記被呼者に暗号化形式で伝達される前に暗号化するように構成された安全ノードとを備え、前記呼経路の少なくとも一部分にわたる通信が暗号化され、かつ前記呼経路の残りの部分にわたる通信が暗号化されていないことを特徴とする交換通信網を介する通信を可能とするシステム。

【請求項6】 前記安全ノードが、交換機と、複数の暗号器と、

## 2

前記の非暗号化情報に前記暗号器のうちの特定の暗号器への経路を設定するために前記交換機を制御する制御手段とを備えたことを特徴とする請求項5記載のシステム。

【請求項7】 前記制御手段が、データベースと、前記被呼者によって使用される暗号の型を判定する手段と、前記暗号型の各々を前記暗号器のうちの特定の暗号器に関係付けて前記データベースに記憶されている情報を検索する手段とを備えたことを特徴とする請求項6記載のシステム。

【請求項8】 交換通信網に配置され、発呼者から非暗号化情報を受信する手段と、前記の非暗号化情報に、対応する暗号化情報を生成するための複数の暗号解読器のうちの選択された解読器を通して経路を与える手段と、前記の暗号化情報を前記被呼者に送る手段とを備えたことを特徴とする安全ノード。

【請求項9】 交換通信網を含む呼経路を介して発呼者と被呼者との間の通信を可能とするために、前記発呼者によって発信され前記被呼者に宛てられ且つ暗号化情報を前記通信網に適用する第1のCPE（加入者構内装置）と、前記交換網に配置されていて、第1の暗号化アルゴリズムを用いる前記CPEから受信した情報を前記第1の暗号化アルゴリズムとは異なる第2の暗号化アルゴリズムを用いて暗号化情報に変換するように構成された安全ノードと、前記安全ノードから前記被呼者に宛てられ暗号化形式の変換された情報を受信する第2のCPEとを備え、前記呼経路の少なくとも第1の部分にわたる通信が第1の暗号化アルゴリズムを用いて暗号化され、かつ前記呼経路の少なくとも第2の部分にわたる通信が第2の暗号化アルゴリズムを用いて暗号化されることを特徴とする交換通信網を介する通信を可能とするシステム。

【請求項10】 前記安全ノードが、交換機と、複数の暗号器および暗号解読器と、前記の暗号化情報に前記の暗号器および暗号解読器のうちの特定のものを通る経路を与えるために前記交換機を制御する制御手段とを備えたことを特徴とする請求項9記載のシステム。

【請求項11】 前記制御手段が、データベースと、前記の第1および第2のCPEで使用される暗号の型を判定する手段と、前記暗号型の各々を前記の暗号器および暗号解読器のうちの特定のものに関係付けて前記データベースに記憶されている情報を検索する手段とを備えたことを特徴とする請求項10記載のシステム。

## 3

【請求項12】 交換通信網に配置され、発呼者から第1の暗号化形式を用いて暗号化情報を受信する手段と、前記の暗号化情報に、対応するクリアな情報を生成するための解読器を通して経路を与える手段と、前記の対応するクリアな情報に、第2の暗号化形式を用いて暗号化情報を生成するための暗号器を通る経路を与える手段と、前記の暗号化情報を前記被呼者に送る手段とを備えたことを特徴とする安全ノード。

【請求項13】 交換通信システムを通る経路が選択される暗号化通信を処理するために、異なる暗号化／暗号解読アルゴリズムを用いて通信を暗号化／解読するようにそれぞれ構成された複数の異なる型の暗号器と、入って来る通信に、与えられた信号メッセージに応じて複数のハント・グループの1つへの経路を与えることにより、前記ハント・グループの何れに経路設定される通信も特定の型の前記暗号器のうちの利用できるものに接続されるように構成されたPBXと、前記の入って来る呼に用いられている特定の暗号化／暗号解読アルゴリズムにしたがって前記信号メッセージを前記PBXに与える手段とを備えたことを特徴とする安全ノード。

【請求項14】 交換通信網を含む呼経路を介して発呼者と被呼者との間で通信を行うために、加入者構内装置(CPE)で前記発呼者により発信され前記被呼者に宛てられ且つ暗号化情報を前記交換通信網に適用するステップと、前記交換通信網に配置された安全ノードにおいて、前記CPEから受信された前記の暗号化情報を、前記情報が前記被呼者に非暗号化形式で伝達される前に解読するステップとを備え、前記呼経路の少なくとも一部分にわたる通信が暗号化され、かつ前記呼経路の残りの部分にわたる通信がクリアであることを特徴とする交換網を介する通信を可能とする方法。

【請求項15】 前記安全ノードが、交換器および複数の暗号解読器を備え、前記方法が、前記の暗号化情報を前記暗号解読器の特定の解読器に経路付けするように前記交換機を制御する制御ステップをさらに含むことを特徴とする請求項14記載の方法。

【請求項16】 前記制御ステップが、前記CPEにおいて使用されている暗号の型を判定するステップと、前記暗号型の各々を前記暗号解読器の特定のものに関係付けながらデータベースに記憶されている情報を検索するステップとを備えたことを特徴とする請求項15記載の方法。

【請求項17】 発呼者から暗号化情報を交換通信網の中に配置された安全ノードにおいて受信するステップと、対応するクリアな情報を生成するために、前記ノードに

## 4

ある暗号解読器を通る経路を前記の暗号化情報に与えるステップと、前記のクリアな情報を前記ノードから前記被呼者に送るステップとを備えたことを特徴とする交換網に安全機能を与える方法。

【請求項18】 交換通信網を含む呼経路を介して発呼者と被呼者との間の通信を可能とするために、前記発呼者によって発信され前記被呼者に宛てられ且つ非暗号化情報を第1の加入者構内装置(CPE)から前記通信網に適用するステップと、前記交換通信網に配置された安全ノードにおいて前記第1のCPEから受信された前記の非暗号化情報を該情報が前記被呼者に暗号化形式で伝達される前に暗号化するステップとを備え、前記呼経路の少なくとも第1の部分にわたる通信が暗号化されず、前記呼経路の残りの部分にわたる通信が暗号化されることを特徴とする交換通信網を介する通信を可能とする方法。

【請求項19】 特定の型の暗号器を用いる発呼者からの情報を交換通信網の中に配置された安全ノードにおいて受信するステップと、対応するクリアな情報を生成するように構成された前記安全ノードにおける複数の暗号解読器の適切な解読器を通して前記の暗号化情報の経路選択を行うステップと、前記のクリアな情報を前記ノードから前記被呼者に送るステップとを備えたことを特徴とする交換網に安全機能を与える方法。

【請求項20】 交換通信システムを通る経路が選択される暗号化通信を処理するために、前記の暗号化通信をPBXに適用するステップと、異なる暗号化／暗号解読アルゴリズムを用いて通信を暗号化／解読するようにそれぞれ構成された複数の異なる型の暗号器の1つに向かい前記PBXを通る経路を前記通信に与えるステップと、入って来る通信に、前記PBXに与えられる信号メッセージに応じてPBX内の複数のハント・グループの1つへの経路を与えることにより、前記ハント・グループの何れに向けて経路設定される通信も特定の型の前記暗号器の適切なものに接続されるステップと、前記の入って来る通信に使用される特定の暗号化／暗号解読アルゴリズムにしたがって前記信号メッセージを前記PBXに与えるステップとを備えたことを特徴とする暗号化通信を処理する方法。

【請求項21】 発呼者と被呼者との間に安全な通信を与えるために、前記発呼者および前記被呼者を接続する通信網においてクリアな通信経路を確立する確立ステップと、安全な通信を開始したいという前記の両当事者のうちの一方による希望を表す信号を検出するために前記通信経路を監視するステップと、前記通信経路の少なくとも一部分の通信をクリアから安

## 5

全に変換する変換ステップとを備えたことを特徴とする安全な通信を与える方法。

【請求項22】 前記確立ステップが、前記発呼者から前記被呼者への呼に対し前記通信網に配置されたインテリジェント交換機を介する経路を与えるステップを含み、かつ前記変換ステップが、前記の一方の当事者によって使用される関係付けられた暗号化装置と互換性のある選択された暗号化装置を前記通信経路に挿入するように前記インテリジェント交換機を制御するステップを含むことを特徴とする請求項21記載の方法。

【請求項23】 前記の関係付けられた暗号化装置において使用される暗号化アルゴリズムの型を確認するために前記の一方の当事者に問い合わせるステップと、前記の問い合わせに対する応答にしたがって前記の選択された暗号化装置を選ぶステップとをさらに備えたことを特徴とする請求項22記載の方法。

【請求項24】 安全な通信を与えたいという前記の両当事者の他方による希望を表す信号を検出するために前記通信経路を監視するステップ、および前記通信経路の残りの部分の通信をクリアから安全に変換するステップをさらに備えたことを特徴とする請求項21記載の方法。

【請求項25】 前記確立ステップが、前記発呼者から前記被呼者への呼に対し前記通信網に配置されたインテリジェント交換機を介する経路を与えるステップを含み、前記変換ステップの各々が、前記の両当事者によって使用される関係付けられた暗号化装置と互換性のある選択された暗号化装置を前記通信経路に挿入するように前記インテリジェント交換機を制御するステップを含むことを特徴とする請求項24記載の方法。

#### 【発明の詳細な説明】

##### 【0001】

【産業上の利用分野】 本発明は、概して、音声、データ、ファクシミリ、ビデオ、およびその他の情報を伴う安全な通信に関する。

##### 【0002】

【従来の技術】 資格のない人々が彼らのためのものではない音声、データ、ファクシミリ、ビデオ、またはその他の情報を傍受しアクセスすることができないように通信システムの安全性を高めることが過去数年にわたり非常に重要視されてきた。研究によれば、商業市場は自らの通信システムに対する脅威に十分気付いており、安全性が崩壊する可能性があるために危険であるようなビジネス・アプリケーションを明らかに意識している。このように関心が高まる理由は多数あり、会話の一部が空中を介して伝えられるために攻撃をより受けやすいセルラ電話の使用の増加、および電気通信網の他の部分---即ち、配線室(wiring closet)、接続箱(junction box)、マンホールまたは電柱の接続、ファクシミリ装

## 6

置、そして特にコードレスおよびセルラ式の電話---が安全の侵害を特に受ける可能性があるという事実もそうである。

【0003】 安全な通信への関心の高まりにもかかわらず、現在の安全技術にはいくつかの制限があり、安全な通信をしようと思うと発呼者も被呼者も暗号化された信号を共通のハンドシェイク・プロトコルおよび暗号化アルゴリズムを用いて送受信することのできる送受信両用の安全装置を備えなければならないという一般的な必要性もその1つである。そうでなければ、安全な通信は通常不可能である。このように、現時点では、セルラ電話を用い、それゆえにより高い安全性を望むような発呼者が適切な装置をしていない被呼者と通信することは一般に困難である。米国特許第4,972,479号(1990年1月20日に付与、発明者;アール・ダブリュー・トビアス(R. W. Tobias))に記述された1つの例外において、この問題の解決を試みてはいるものの、加入者の構内に置かれた呼迂回装置を伴う複雑かつ非経済的な方法で行っている。別の状況では、セルラ電話の利用者は、移動電話交換局と暗号モードで通信することができ、移動電話交換局(MT S O=mobile telephone switching office)は、目的先への呼をクリアな(即ち、非暗号化)モードで完成させる。しかしながら、この種の構造の有用性には限度があり、MT S OへのアクセスがそのMT S Oのサービス範囲に物理的に位置する発呼者に限られていて、この範囲外の発呼者がMT S Oの暗号設備を利用することはできない。さらに、MT S O環境において現在使用されている暗号構造では、1つの暗号アルゴリズムから別のものへの変換、および音声の呼以外の通信がサポートされていない。

【0004】 同様に、呼の発信者が安全な(即ち、暗号化可能な)電話を持っていない場合、それへの帰属が微妙と思われる領域において呼を受信している側が暗号化された情報を自らの局所的電話リンク(例えば、終端の中央局から加入者の構内まで)で受信することを保証することは一般に不可能である。さらに、仮に発呼者および被呼者の両方が安全な電話を持っていても、互いに正しく通信するためには、両者は、同じプロトコルおよびアルゴリズムを使用しなければならない。

##### 【0005】

【発明が解決しようとする課題】 発明が解決しようとする課題は、呼の当事者の双方がハンドシェイク・プロトコルおよび暗号アルゴリズムの異なる安全装置を有する場合、または当事者の一方のみが安全装置を有する場合、安全な通信を行うことができないことである。

##### 【0006】

【課題を解決するための手段】 本発明によれば、第1のフォーマットで暗号化された情報(これは、音声、データ、ファクシミリ、ビデオ、およびその他のタイプの呼またはメッセージでもよい)を(a)異なるフォーマッ

トで暗号化された情報、または(b)非暗号化情報に変換したり、またはこの逆の変換をするように構成され、かつ発呼者および被呼者を接続する通信網に配置された安全なノード(以下において、「安全ノード」と称する)を用いることによって、両当事者の間で安全な通信を行うことができる。発呼者により発信され、前記の安全ノードを介して被呼者に送られる呼またはメッセージの経路選定を行うことによって、情報は、伝送経路の両当事者間の部分だけが暗号化され、伝送経路の他の部分は暗号化されないことがある。また、異なる暗号化アルゴリズムを用いて経路の異なる部分で情報が暗号化されることもある。これにより、発信端または終端において一方の当事者のみが安全装置を有する場合でも、通信路の安全でない部分への攻撃は可能であるがその可能性は小さいので、当事者は、比較的安全な通信が得られるサービスを受けることが可能となる。また、本発明では、異なるハンドシェイク・プロトコルおよび暗号化アルゴリズムによる安全装置を使用する当事者の間でも安全な通信が許される。安全な網サービス・ノードは一度に多くの利用者にアクセスされることがあるので、このサービスに関する費用は分担して小さくすることができる。

#### 【0007】

【実施例】図1は、本発明によって構成された安全ノード150の構造、および市内通信網および相互交換通信網の種々の要素とその構造との関係を示す。安全ノード150は、(a)伝送経路のある部分(例えば、発呼者とノード150との間の部分)で伝達される情報は安全にできる(暗号化できる)が、伝送経路の他の部分(例えば、ノード150と被呼者との間)で伝送される情報はクリアである(暗号化されない)ような通信、または(b)発呼者とノード150との間の伝送経路の部分で伝達される情報が第1の暗号化アルゴリズムを用いて暗号化できる一方、ノード150と被呼者との間の伝送経路の部分で伝達される情報は第2の異なる暗号化アルゴリズムを用いて暗号化されるような通信を達成するように設計される。

【0008】図1において、近い側の加入者構内装置(CPE)101を使用している発呼者によって発信された通信は、遠い側のCPE102を使用している被呼者に宛てられ、またこの逆の場合もある。ここで用いる場合、「通信」には、音声、データ、ファクシミリ、ビデオ、またはその他の情報を伝えるアナログまたはデジタルの呼またはメッセージを含めても良い。以下において、通信を単に呼と称することがある。CPE101および102は、それぞれ市販の安全電話ユニット(STU)---例えば、AT&Tより入手可能なSTU-III電話、またはモトローラ(Motorola)もしくはジェネラル・エレクトリック(General Electric)のような販売会社から入手可能な別の安全端末など---を備えてもよい。あるいはまた、CPE101および(または)CP

E102が、それぞれ安全電話装置(STD)191、192、即ち、関係付けられた電話193、194、またはファクシミリ装置、データ端末または他の通信装置へと接続する付属装置を備えても良い。尚、CPE101またはSTD191がCPE102またはSTD192と同じ種類である必要はなく、事実、異なる暗号化アルゴリズムやハンドシェイク・プロトコルを用いる異なる製造業者から入手することも可能である。また、CPE101またはCPE102の(両方ではなく)一方は、普通の(安全でない)端末または装置でもよい。

【0009】以降の説明のために、CPE101は、クリアか安全かを問わず出て行く(即ち、発呼者から安全ノードへの)呼および入って来る(即ち、安全ノードから被呼者への)呼を送受信するように構成されているものと仮定する。CPE101の交換機により、装置が動作するモード(クリアまたは安全)を制御し、モードの変更は、交換機を操作することにより利用者の直接制御の下で局所的に行われたり、遠隔地で生成された信号に応じて行われたりする。データの入力を便利にするために、CPE101にタッチ・トーン発生器およびキーパッドを備えて、LED表示ランプなどの表示指示器によって状態を利用者に示すことができる。安全からクリアの通信を最初に説明するので、すぐ後の説明のために、CPE102が通常の電話機であると仮定する。

【0010】安全ノード150への通信「アクセス」は、(a)ソフトウェアで定義されたネットワーク(SDN)アクセス番号、または(b)AT&Tから利用可能なMEGACOMのようなプレミアム・サービスに関連した普通の旧式の電話サービス(POTS=plain old telephone service)番号、または(c)800番を使用するなどの便利なアクセス機構によって得ることができるが、説明のために、CPE101を使用する発呼者は、1-800-ENCRYPTのような所定の料金無料番号をダイヤルすることによってノード150へのアクセスを得るものと仮定する。この番号にダイヤルすると、呼は、発呼者を管轄する市内交換キャリア(LEC)局108にある交換機107(例えば、AT&Tから入手可能な電子交換機#5ESS(登録商標))を通して、総括的に156として指定される交換通信網の一部である相互交換キャリア交換機110(一般に、AT&Tの#4ESSアクション・コントロール・ポイント(ACP))へと経路選択されて送られる。交換機110は、これに応じて、信号メッセージを(通常はCCS7信号フォーマットで)生成し、これを相互に接続された複数の信号転送点(STP=signal transfer point)116、117を含む共通チャネル信号(CCS)網115を通して、発呼者の加入計画により着信ワッツ(InWATS)データベース(IDB)120またはソフトウェアで定義されたネットワークにおける網制御点(NCP)へと経路選択して送る。IDB120は、ダイヤルされ



たそれぞれの800番に対するレコードを収容し、ダイヤルされた番号に関係付けられた経路選択番号（これは、交換機110に送り返される）を生成するために参照動作を行う。次に、交換機110は、経路選択番号に応じて、その呼を安全ノード150へと経路選択して送るが、通常は交換通信網156の他の構成要素を通して送り、このとき別の#4ESS交換機125を含んでも良い。また、LEC局108には発呼者を図1に示したように直接接続しても、PBX交換機または他の加入者構内装置（CPE）（図示せず）を介して接続しても良い。さらに、CPE101と安全ノード150との相互接続には、他のアクセス構造および信号構造を使用しても良い。

【0011】安全ノードにおいて呼が受信されると、そのノードは、ダイヤルされた番号およびCPE101を識別する自動番号識別（ANI）情報が入ったCCSメッセージも交換機107、110、または125から受信する。しかしながら、そのような情報の利用可能性は、LEC局108およびネットワーク156によって使用されている交換機および信号装置の能力に依存する。次の説明のために、発呼者の情報は発呼者に催促することなしには利用できないものと仮定する。

【0012】図1に示したように、安全ノード150は交換機151を備えている。この交換機は、例えば、AT&Tより入手可能なDefinity（商標）デジタルPBXであり、トランク160上で受信した入接続呼を線群161の中の1つの線を介して交換機コントローラ152の利用可能なポートに接続するように構成されている。また、交換機151は、呼を線群164経由で暗号器バンク170の中で利用可能な暗号器に接続するように構成されている。コントローラ152は、例えばAT&Tより入手可能なConversant（登録商標）システムであり、内部のデータベース（DB）154に記憶された原稿に従って発呼者に音声のプロンプトを送信できる音声応答ユニット（VRU）153を含む。また、コントローラ152は、それ自体でまたは交換機151と連携して他の種々の機能を果たす。例えば、プロンプト送信に応じて発呼者が入力した情報を受信し、これをデータベース164から検索した情報との関連において論理的な処理をすることができる。このような情報は、通常CPE101の一部であるタッチ・トーン・ダイヤル・パッドを用いるか、またはキーボードもしくは他の別個の入力装置によって、発呼者が入力することができる。場合によっては、情報を音声の応答として入力し、「音声からテキストに」処理する機能を用いて翻訳できることもある。さらに、コントローラ152は、交換機151と連携して、（a）ダイヤル数列を生成して交換機151に適用することによって呼を開始する（または開始するように交換機151に指示する）こと、（b）いくつかの入力で呼を同時に受信し処理すること、さらに（c）

入接続呼および出せつぞく呼を共にブリッジする（またはブリッジするように交換機151に指示する）ことが、可能である。また、コントローラ152は、発呼者または被呼者によって呼経路に印加される制御信号を検出し、それに基づいて動作するために所定の時間または期間だけ呼経路に留まることができる。以上の機能は、前記のConversantシステムおよび他の業者より入手可能な同様のシステムにおいてもすべて利用することができる。

10 【0013】安全からクリアの通信（即ち、CPE101と安全ノード150との間の安全、およびその安全ノード150と被呼者との間のクリア）を実現しようとしてノード150の番号（例えば、1-800-ENCRYPT）をダイヤルした発呼者から呼を受信した場合に、コントローラ152において取られる処置を図2に流れ図のかたちで示し、次のように要約する。

20 【0014】呼の受信時（ステップ201）に、交換機コントローラ152は、その呼の完成に必要な情報を求めて発呼者にプロンプトを出す（ステップ203）。この情報には、発呼者が加入者であることを確認する「ログイン」などの情報、発呼者の同一性を確認する「パスワード」などの情報、および例えばCPE102の電話番号などの被呼者を識別する情報も含まれる。

30 【0015】処理におけるこの時点において、発呼者によって用いられる暗号の種類を識別する情報も音声プロンプトに応じてコントローラ152で受信することがある。しかしながら、暗号化を開始する前に交わされる「安全伝送開始」信号に暗号の種類を示す符号を含めることなどによって前記の情報の提供を自動化する方が好ましい。しかし、さらに詳細に後述するように暗号の種類は後続の設定過程のある時点で得るようにしてもよい。以下の説明のために、暗号の種類はステップ206において獲得して、データベース154に格納するものと仮定する。異なる暗号化アルゴリズムを取り入れて使用する種々の異なるCPEを使用する加入者を支援するようにノード150が構成されているので、いずれの場合も「種類の情報」は必要となる。従って、ノード150において適切な処理を実施するためには、発呼者によって使用される暗号の特定の種類の詳細が必要となる。

40 【0016】コントローラ152は、発呼者入力情報を受信すると、その発呼者が資格のある利用者かどうかを知るためにデータベース155を調べる（ステップ207）。資格がない場合、コントローラ152は、ステップ209において終了の告知を行うのに対し、資格がある場合、残りのプロンプトに応じて入力される情報を続けて収集する。さらに、コントローラ152は、課金処理を開始するために発呼者の識別情報および被呼者の情報を記録/課金プロセッサ185に送る（ステップ211）。プロセッサ185は、以降の一連の課金のために呼の詳細を記録している自動課金評価/書式化システム

11

187と周期的に通信を行う。呼の詳細には、通話の日付、時刻および長さ、呼び出された番号などが含まれる。課金処理を、ノード150に關係する呼設定および暗号化の「主な」処理とは関わりなく続くように図2に示す。

【0017】コントローラ152が、CPE101において使用されている暗号の型を判定すると、CPE101で生成された暗号化された信号を効率的に処理（即ち、解読）できる暗号アルゴリズムを使用する暗号器バンク170のバンク内部で選択された暗号器に關係付けられたハント・グループの指定を判断するためにデータベースの参照動作が行われる（ステップ215）。同じ暗号型を用いている呼は幾つか同時に処理することができるので、暗号器バンク170には、そのようないくつかの暗号器が含まれ、それらの各々が同じハント・グループにおいて個別のアクセス番号を持っている。

【0018】次に、コントローラ152は、発呼者によって使用されている選択された暗号の型に關係付けられたハント・グループを表す制御信号（一般に、トーン信号）を交換機151に結合する。ハント・グループが呼び出されると、次に利用可能な適切な型の暗号器（例えば、図1の暗号器172）が交換機151によって選択される。しかし、選択された型の暗号器が利用できない場合（ステップ217）、処理は終了する（ステップ209）。

【0019】特定の暗号器が選択された場合、（CPE101において生成された呼に関する）その入力端が、導線164によって交換機151に接続される（ステップ219）。順方向、即ちCPE101からCPE102の方向には、実際に暗号器172は、CPE101で暗号化された呼を解読するように動作して、呼はCPE102からノード150までクリアに展開することができる。

【0020】暗号器バンク170の中の暗号器はそれ自体に通信信号能力はほとんど備えていないので、暗号器172を含む各暗号器は、信号処理をコントローラ152によって行うことができるように暗号器の（CPE101で生成された呼に関する）出力端が交換機151の導線側の端に接続されるように構成することができる。具体的には、暗号器172が選択されると、その出力端は、交換機151の導線165に接続され、これによって、ダイヤル・トーンがコントローラ152に供給される。

【0021】交換機コントローラ152は、ダイヤル・トーンを受信すると、これに応じて交換機151に加えられるダイヤル・トーンを生成し、その交換機にコントローラ152への第2の呼を開始させる（ステップ221）ように構成される。この呼（導線166を介して交換機151からコントローラ152に展開される）は、呼設定処理が完了した後にコントローラがクリア・モー

12

ドの（即ち、非暗号化）呼を引き続き監視できるようにするので、望ましいものである。さらに詳細に後述するように、コントローラ152による第1の接続（呼の設定が完了した後、切断される）により、コントローラが呼の道筋にあたる位置に置かれるので、（クリアではなく）暗号化された音声／データが受信される。

【0022】ここで、コントローラ152は、CPE102の呼を完成させる位置にある。呼を完成させるために、入接続呼（即ち、CPE101から暗号器172を介してコントローラ152に至る呼）を保留し、以前に与えられデータベース154に格納されていた被呼者の番号への新たな呼を開始する（ステップ223）。この呼の経路は、コントローラ152から交換機151へ導線168を介して与えられる。この呼は、交換機151からトランク163を介して交換機125に経路付けされ、さらに通常の呼設定および信号授受の手順を用いて通信網経由で意図する伝送先のCPE102まで経路付けされる。安全ノード150から被呼者への出口は、SDN（ソフトウェア定義ネットワーク）のMEGACOM（登録商標）またはその他のサービス（AT&Tから入手可能なPROWATS、WATS即ちビジネス長距離）によって与えられる。通信網156とCPE102との間の通信は、一般に第2のLEC局（終端用の#5ESS交換機111を備えている）によって行われる。

【0023】発呼者が応答すると、応答指示が交換機125で検出され、交換機151を通してコントローラ152に渡される。コントローラ152は、これに応じてコントローラ152への呼（導線161上）をコントローラ152からの呼（導線162上）にブリッジするように交換機151に合図するように構成されている。これにより、コントローラ152の「出現」が呼経路から1つ除去されるが、第2の出現がそのまま残る。これによって、コントローラ152は、端から端までの接続が行われた後、制御信号（タッチ・トーン信号または音声で、暗号化されているものよりクリアなものが多い）の発生を知るために引き続き呼を「監視」することができるので、呼の進行中に以下に述べる他の何らかの動作を行うことができる。

【0024】逆方向、即ち被呼者（CPE102）から発呼者（CPE101）への通信は、呼経路が交換機151で一旦設定されると、同じ経路をたどり、戻りの方向に対する（暗号解読ではなく）暗号ユニットとして暗号器172を使用する。

【0025】発呼者とノード150との間の安全な通信を実現するために使用されるトレーニング・シーケンスを説明する前に、呼の設定過程を図3に関連した別の形式で説明する。図3において、図1にある構成要素に対しては同じ表示を使用しているが、呼の流れは「直線的に」示してある。即ち、交換機151およびコントローラ152が複数回現れるのを一括していない。

【0026】図3において、CPE101によって開始された呼は、例えば交換機107、110および125を含む市内および市外の通信網（図3には図示せず）を通る経路により送られ、交換機151の第1の入力ポート301に達し（ステップ201）、さらにこれにより、その出力ポート302を介してコントローラ152の第1の入力ポート311へと経路選択されて送られる。CPE101において行われる暗号化の種類を判定するために十分な情報をコントローラが得た後（ステップ203、205）、コントローラ152によって暗号器バンク170にある暗号器の中の1つ（例えば、暗号器172）に接続が行われる（ステップ207、215、217）。この接続は、（1）コントローラ152によってその出力ポート312において交換機151の利用可能な入力を捉え、かつ（2）適切な種類の暗号器に関係付けられたハント・グループ番号をダイヤルすることによって、行われる。この接続により、交換機151は呼を出力ポート304から暗号器172へと経路付けして送る（ステップ219）ことになる。

【0027】暗号器172の出力側は、交換機151の入力ポート305に接続され（ステップ221）、これによって、ダイヤル・トーンがコントローラ152に送り返される。コントローラ152は、このダイヤル・トーンの受信に応じて、呼をその着信先に接続するために必要な信号（即ち、各桁の数字）をポート312からコントローラ152を通る第2の接続によって出力する（ステップ223）。この接続を確立する方法は幾つかあるが、次の手順が好ましい。まずポート312からのデジタル出力により交換機151に呼を開始させることにより、その入力ポート305を出力ポート306に接続し、この出力ポートはコントローラ152の第2の入力ポート313に接続される。コントローラ152は、出力信号（数字）を受信し、ダイヤルされた番号を表す制御信号を出力ポート314から交換機151の利用可能な入力ポート307に与えることにより新たな呼を交換機151によって開始する。この呼が開始されるのは、交換機151がポート307を交換通信網における交換機125に接続された出力ポート308に接続するときである。

【0028】CPE102を使用する被呼者から応答指示を受信すると、CPE101からノード150を通して被呼者のCPE102までクリアな通信路が形成される。この時、コントローラ152は、交換機151にポート301における呼の入力をポート304における呼の出力と共にブリッジするように合図する（ステップ225）。これにより、コントローラ152が1回出現する周囲にバイパスが設置されるが、呼を監視し（ステップ227）、制御信号または呼ステータスの状態を検出し、これに応じて、他の種々の呼設定および（または）維持機能を実行するために、このコントローラの第2の

出現が呼経路のクリアな部分に残ることが許される。

【0029】図2との関連で説明した処理により、CPE101とCPEセル102との間に安全なノード150によるクリアな通信路が設置される。呼の期間中に時として、発呼者がCPE101とノード150との間の呼の部分を暗号化することに決めることがある。CPE101と安全ノード150との間の通信をクリアから暗号化へと切り替えることを可能にするトレーニング・シーケンス処理を図4に示す。同図は、図3に関して続けて読むべきである。発呼者は、暗号通信を始めたいと思った場合、その意図を着信側に知らせたのち、例えばCPE101の「安全通話」ボタンを押す（ステップ401）などによりCPE101内部の暗号ユニットにきっかけを与えてモデム・トレーニング・メッセージに似たメッセージを暗号器バンク170の暗号器172に送らせる（ステップ403）ことによって安全ノードへの転送を開始する。これに応じて、暗号器172は、モデム応答信号をCPE101に送る（ステップ405）。暗号器172に関するトレーニングが進行中であることを示すために、CPE101における何らかの表示、例えば、安全発呼ボタンに関係付けられた点滅する（安全）指示灯などを用いてもよい。

【0030】初期のトレーニングが完了すると、安全な通信の確立の準備として周知のデータ通信プロトコルを用いて、キー交換シーケンスが開始される（ステップ407）。そのようなデータ通信プロトコルの1つが、ANSI規格X9.17にも説明されているが、その他の多数の技術が当業者には周知である。必要であれば、暗号トレーニング中にコントローラ152によって発生される告知を被呼者で受信することもできる。CPE101は、キーの交換が順調に完了すると直ちに安全指示灯が点滅を中止して光った状態を維持するように、構成してもよい。また、コントローラ152は、キー交換シーケンスの処理の完了を検出し、呼が安全モードに移行することを示す告知が発呼者に対して再生されるようにしてもよい。ひとたび安全モードになると、その呼の流れは、その呼の期間中、暗号器172およびコントローラ152を通り続ける（ステップ411）。

【0031】発呼者が安全モードからクリア・モードに変更したい場合、例えばCPE101のクリア・ボタンを押す。この信号は、暗号器172で検出され（ステップ413）、これに応じて、暗号器がクリア・モードに移る。このクリア・モードへの転換は、呼をクリア・モードに転換する要求の合図をするべく、例えば暗号化されたデータには通常発生しないような独特のデータ・パターン（例えば、00110011001100110011...のような繰り返しパターン）をCPE101が送る（ステップ415）ことによって実現される。暗号器172は、この独特なパターンを検出し、クリア・モードに切り替える要求をCPE101から受信したことを示すために、同じように

000111000111のような別の独特なボタンによって応答する。次に、CPE101が、暗号器172によって返された信号に例えば0101010101010...などの第3の独特なボタンで応答して安全からクリアへのハンドシェイクを完了する(ステップ417)。このハンドシェイク処理は使用可能なプロトコルを説明するためのものであるが、その他の方法も当業者には明かである。その後、終了信号または切断信号が検出されるまで、呼は継続する(ステップ419)。

【0032】発呼者および被呼者が異なる種類の暗号器／解読器を使用している場合、即ちCPE101およびCPE102が同じ暗号化アルゴリズムを使用していない環境において、両者の間で安全から安全の呼を行う時にも、本発明は使用することができる。この実施例では、暗号器バンク170において利用可能な2つの暗号器を用いることにより、安全ノード150が互換性のない暗号化／解読装置の間に暗号変換を与えている。

【0033】ノード150における暗号変換によって安全な呼を発信するために使用される処理を図5に流れ図の形式で示す。この処理における最初のステップは、安全からクリアの呼に関連して既に説明したものと同じであり、従って、図2の処理を最初に行い、CPE101とノード150との間の安全経路およびノード150からCPE102までのクリア経路を確立する。図6は、この種の呼に必然的に含まれるハードウェア要素を例示するもので、以下の説明の参考になる。

【0034】呼経路の第2の区間(即ち、ノード150から被呼者の場所にあるCPE102まで)の通信もクリアであるより暗号化されるべきときには、通常、被呼者によってコントローラ152に合図が送られる(ステップ501)。(しかしながら、構造によっては、呼の両方の区間を暗号化するという判断がCPE101を使用する発呼者またはCPE102を使用する被呼者の一方によって合図されるものもある。)コントローラ152は、呼経路に第2の暗号器が必要であることを示す制御信号を検出すると、使用されている暗号器の種類を判定するためにCPE102に照会する(ステップ503)。この問い合わせにより、暗号器バンク170から適切な(第2の)暗号器を選択するために必要な情報がコントローラ152に与えられる。

【0035】コントローラ152は、コントローラ152を通る経路が設定される第2の呼を確立するように信号を第2の出力ポート(図6におけるポート315)から交換機151に送る(ステップ505)。多くのPBX交換機は現在のところ出接続呼の「転送」も「ブリッジ」もできず、入接続呼の転送またはブリッジしかできないので、この構造を使用する。また、この構造を用いるのは、呼経路のうち通信がクリアな部分にコントローラ152を残すためでもある。このことは以下において十分説明する。尚、図6において、コントローラ152

への第2の呼はポート315に端を発し、交換機151の入力ポート601に至り、この交換機により、その出力ポート602を介して異なる入力ポート611にてコントローラ152に接続される。

【0036】コントローラ152により、CPE102における発呼者によって使用されている特定の暗号器の種類に関係付けられたハント・グループを特定する情報をデータベースの参照を用いて決定する(ステップ507)。次に、コントローラ152は、コントローラ152のポート612から出力され交換機151の入力ポート603に加えられるハント・グループに関する番号への呼を開始し、適切な暗号器が使用できると交換機が判断した場合(ステップ509)、交換機が暗号器バンク170における適切な種類の次に利用可能な暗号器(例えば、図6における暗号器174)に呼を接続する(ステップ513)ようにさせる。利用できないと判断した場合、ステップ511において終了メッセージを再生する。

【0037】暗号器174は、暗号器172と同様に、その出力が交換機における回線側の終端(ポート605)に接続されるように構成されている。しかし、この例では、暗号器174も、交換機151の出力ポート606からコントローラ152の異なる入力ポート(ポート613)への間の交換機151における接続を実施するために必要な信号が暗号器174が動作状態になった時に常に生成されるように、構成されている。これは、暗号器バンク170のいくつかの暗号器を交換機151における「仮想的な直通回線」接続(暗号器がその入力ポートで呼を受信することにより動作状態になったときコントローラ152の利用可能なポートに自動的につながる)に接続されるように調整することによって、実現される。仮想的な直通回線は、交換機151の回線側の1つ以上の終端のオフ・フック状態を検出するように交換機151をプログラムし、オフ・フック状態の検出時にコントローラ152またはCPEからの合図をさらに必要とすることなく呼を自動的にプログラムされた目的点に経路設定することによって実施される。

【0038】コントローラ152が「直通回線」の呼をポート613で受信すると、その入力ポート313間の接続を出力ポート314から出力ポート315へと切り替える(ステップ517)ようにコントローラ152を調整する。同時に、ポート613および314がコントローラ152の内部で接続され、ポート602および604が交換機151の内部で接続される。この状態における呼経路を図7に示す。次の点に注目する必要がある。

【0039】(a)呼経路に2つの暗号器172および174があり、第1の暗号器はCPE101から受信される暗号化されたメッセージを安全な形式からクリアな形式に変換するのに適した型のものであり、第2の暗号

器はCPE102から受信される暗号化されたメッセージを安全な形式からクリアな形式に変換するのに適した型のものである。

【0040】(b)暗号器「172および174の間の呼経路のクリアな部分にコントローラ152が残る。従って、必要ならば、回線の両端の当事者によってコントローラ152に信号を送ることができる。

【0041】図5の処理は、制御信号または終了信号を求めて呼を監視する(ステップ519)ことにより完了する。既に説明した実施例の場合のように、呼の終了は、CPE101またはCPE102の何れかがハンドセット(送受器)を置いたときに通常どおり実現される。この場合、切断信号が交換機151またはコントローラ152によって検出され、接続が取り払われる。

【0042】図8において、CPE101は安全な音声端末であり、通常の可聴周波入力(マイクロフォン)および可聴周波出力(拡声器)を備えたハンドセット800はハンドセット・インタフェース801に接続され、線802でアナログ信号(200から3000Hz)を送受信する。外に向かう信号(CPE101で生成され交換機107を介して被呼者に送られる信号)については、インタフェース801の出力はアナログ/デジタル変換器803に接続され、そこで、可聴周波帯域信号が例えば56Kbpsの標準化され且つ量子化されたパルス符号変調(PCM)デジタル信号へとデジタル化される。このようにするのは、CPE101ではデジタル処理の方が好ましいからである。

【0043】アナログ/デジタル変換器803の出力は、音声符号器/復号器(音声コーデック)805に加えられる。コーデック805は、受信したビット・ストリームをデジタル・ワード・ストリームに一般に2400bpsで圧縮する。圧縮の一種として、AT&Tから入手可能なSTU III安全音声端末に見られる種類の符号励起線形予測(CELP)符号器/復号器がある。この圧縮符号化を行うのは、暗号作成モジュール807において実行される暗号化/暗号解読を容易にするためである。このモジュールは、記憶されている暗号キーを用いてクリアなデータと安全なデータとの間で周知の翻訳を行うように構成される。暗号化の本質は、暗号キーにアクセスする資格を有する利用者のみに安全なデータを解読することを許し元の情報を再生できるようにすることである。暗号作成モジュールの一例は、連邦情報処理規格(FIPS)140-1「暗号作成モジュールに対する安全条件(Security Requirements for Cryptographic Modules)」の1990年7月付けの草案に説明がある。

【0044】暗号作成モジュール807の出力は、モデム809へ、そしてD/AおよびA/D変換器811へと加えられるが、両者は、共に信号路に挿入され、暗号作成モジュール807から出力された2400bpsのデ

ジタル信号をアナログ電話回線上の伝送に適したアナログ・モデム・トーンのシーケンスへと変換することを目的とする。モデム809自体が、2400bpsのモデム出力を例えば56kbps(これは、デジタル電話回線への応用に適している)のデジタル・ビット・ストリームへと変換する。このビット・ストリームは、可聴周波トーンを表す。信号が暗号化(スクランブル)されているので、トーンは、資格のない聴取者の場合、元の音声メッセージに含まれている情報を判断することができないようにスクランブルされる。

【0045】CPE101は一般にLEC交換機107への通常のアナログ加入者アクセス・ループを通して電気通信網に接続されるので、モデム809の出力は、電話回線インタフェース813を介して前記のループに加えられる前にD/AおよびA/D変換器811においてデジタル形式(56kbps)から元のアナログ形式に変換される。デジタル・アクセスが提供されている場合には、D/AおよびA/D変換器811、インタフェース813、またはこれらの両方とも必要でないこともある。

【0046】中に向かう信号(安全ノードで生成され、交換機107を介してCPE101に向かう信号)についても同様の変換が行われる。具体的には、スクランブルされた可聴周波トーンを表すアナログ入力、インタフェース813を介して受信され、D/AおよびA/D変換器811でデジタル形式に変換される。一連のアナログ・トーンを表すPCMのビット・ストリームは、モデム809において(例えば)2400bpsのビット・ストリームに変換され、暗号作成/解読モジュール807で解読され、コーデック805において記号がデジタル・ビット・ストリームに変換され、元のアナログ信号を表す。デジタル・ビット・ストリームは、変換器803において理解できるアナログ形式に変換されてから、最終的にインタフェース801を介してハンドセット800に加えられる。

【0047】図8に示したCPE構造は、前面パネルインタフェース回路820も備え、この回路によって、クリア・ボタン821、安全ボタン824、およびキーパッドまたはその他の入力装置822からの入力を受信し、さらにこの回路は、LED、LCDまたは類似の表示装置によって与えられるような視覚的表示を動作させるように構成される。インタフェース820で受信される入力、メモリ840に記憶されたプログラムの制御下で動作するマイクロプロセッサ830において局部的に処理される。また、マイクロプロセッサ830は、D/AおよびA/D変換器803、811、コーデック805、モデム809、さらに大抵の場合暗号作成/解読モジュール807の動作と相互に作用しあい、それらの動作を制御し、かつそれと協調するようにプログラムされる。この後者の相互作用には、キーの記憶/検索、お

およびその他の暗号関連の機能が含まれる。

【0048】図8では、暗号化／暗号解読の要素および関係する信号の変換が電話局に対して内部的に行われるCPEを考察するが、構造によっては、通常の端末に先に説明したような機能を与えるために、通常の端末に

「安全電話装置（STD）」として周知の外部装置を取り付ける方が好ましいこともある。この構造では、STDはハンドセットと電話ベースとの間の利用者の電話機に取り付けられる。別個のACトランスによりSTDに電力を供給する。STDは、多くの種類の電子的、モジュラー式、かつ押しボタン式の業務用および家庭用の電話機と互換性がある方が好ましい。必要に応じて、利用者は、STD上の表示装置およびソフトウェアで定義されたスイッチによってSTDの仕様を変更することができる。このような表示装置によって、安全またはクリアのモードの確認、および通信が無資格者によって変更されていないことを保証する視覚的信号を利用者に与えられる。STDは携帯できるほど十分に小型かつ軽量にすることができるので、都合良くいろいろな場所（例えば、仕事場、自宅、旅行先など）に持ち運ぶことができる。

【0049】図9において、コーデック805、暗号作成／解読モジュール807およびモデム809などの多くの要素は、図8に関連して説明したものと同一である。しかしながら、各暗号器は、一般にPBX、即ち交換器、特に図1のデジタル・スイッチ151からの入力を受信し、かつそれに出力を供給する。この理由から、アナログからデジタルへの変換は必要ないので、D/AおよびA/D変換器803および811が無い。さらに、ハンドセット・インタフェース801および電話回線インタフェース813によって行われる機能は、1対のPBXインタフェース回路901、913によって実行される。

【0050】また、図9の暗号器には、図8の前面パネルインタフェース820の代わりに信号インタフェース920が含まれる。これは、暗号器が都合良く電気通信網の中に位置し、かつ発呼者および被呼者によってコントローラ152の機能を用いて信号が送られるためである。

【0051】先に説明した呼の発信シーケンスは説明のためのものであり、当業者であれば電気通信網の他の構成要素に付加的な知能を組み込む場合に利用可能な種々の代替的な処理が分かるであろう。一例をあげる。図1のデータベース120は、選択された発呼者および被呼者の番号に関する付加的な情報を取り出すことができ、交換機110および（または）125は、信号網115を介して受信される情報に応じて対話的なシナリオを実行できるものと仮定する。この実施例において、発呼者が安全ノード150のアクセス番号をダイヤルすると、その呼は、特殊な処理を必要とするものとデータベース

120によって認識される。発呼者は、例えばその呼の種類、即ちその呼が安全からクリアの呼か、クリアから安全の呼か、または安全から安全の呼かを明確にするように交換機110によってプロンプトが出される。安全からクリアの呼の場合、発呼者は、CPE101上のタッチトーン・パッドを用いて利用者のID番号を入力するようにプロンプトが与えられる。交換機110は、データベースと連携して、利用者のID番号の正統性を確認しようとする。利用者のIDが確認できない場合、利用者は、この状態の通知を受け、正当な利用者ID番号を入力し直すように求められる。試行を2回行った後も、利用者のID番号の正統性が確認できない場合、利用者は、問題があるとの通知を受け、さらに支援を受けるため別の電話番号でサポート・センターに電話するように求められて、呼が取り除かれる。このように、図2のステップ203、205、および207の部分は、ノード150の外側で実行してもよい。

【0052】図1のシステムを用いて安全からクリアの呼を確立する代案の過程を図10の流れ図および図11～15のハードウェア図で説明する。（クリアから安全の呼、および安全から安全の呼に対しても同様の過程をたどる。）この過程は、いくつかの重要な点において前記のものとは異なる。第1に、発呼者および被呼者との間で端から端までの接続が確立されてから、呼経路に暗号器が挿入される。第2に、暗号化が始まると、コントローラ152が呼経路から削除される。第3に、当事者の何れかが安全な通信の開始を希望すると、暗号器の「型」の情報がノード150に自動的に与えられる。

【0053】呼の受信に応じて処理が開始し（ステップ1001）、これに基づいて、交換機コントローラ152は、呼の完成に必要なログイン、パスワード、および被呼者の番号の情報を求めて発呼者にプロンプトを出す（ステップ1003）。暗号器の「型」の情報は、この時点では与えられない。情報が収集され（ステップ1005）、データベース154に記憶される。発呼者が有資格利用者である場合（ステップ1007）、コントローラ152は、（CPE101からの）入接続呼を保留し（ステップ1015）、ステップ217においてCPE102への呼を開始するために先にデータベース154に記憶された被呼者の情報を交換機151に送る。図2の処理の場合のように、この呼の経路は、コントローラ152から線168を介して交換機151へ、交換機151からトランク163を介して交換機125へ、さらに電気通信網を通してCPE102へと至る。発呼者が資格ありと認められた場合、課金および請求処理が開始され（ステップ1011および1013）、発呼者が資格ありと認められない場合、終了の告知が再生される（ステップ1009）。

【0054】被呼者が応答すると、コントローラ152は、コントローラ152への呼をコントローラ152か

らの呼にブリッジするように交換機151に信号で合図する。これにより、両当事者の間にクリアな通信路が確立され、その通信路にコントローラ152の1つの「出現」が一時的に残されるので、そのコントローラ152により、何れかの当事者が呼をクリア・モードから暗号化モードに移すように希望していることを示す制御信号の発生を求めて呼を引き続き「監視する」(ステップ1021)ことができる。

【0055】ステップ1023において、何れかの当事者がその当事者のCPEとノード150との間の伝送路の部分を送信される情報の暗号化を望んでいることを示す「安全伝送開始」の信号をコントローラ152に送った判断される場合、そのCPEで使用されている暗号器の種類が判定が行われる(ステップ1025)。この判定は、コントローラ152によって「自動的に」行われ、このときコントローラ152は、「安全伝送開始」信号と一緒に送られる暗号の型を表す符号を認識する。「安全伝送開始」信号が検出されるまで、ステップ1021が繰り返される。

【0056】トレーニング・メッセージは、発呼者によって使用されている暗号化装置の型を指定するDTMFトーンまたはその他の信号情報を含む。また、交換機151にある付属交換機アプリケーション・インタフェース(ASA I)により、呼の設定中にCPE101において発生されたDTMFトーンを認識することができる。この場合、暗号器の型だけでなく、その型の暗号器に関係付けられたハント・グループ番号(複数可)も自動的に決定して、コントローラ152に送ることができる。

【0057】ステップ1025には、適切な暗号器に対する「ハント・グループ」の決定も含まれる。具体的には、コントローラ152が「安全伝送開始」信号を発したCPEで使用されている暗号器の型を判定したときに、データベース154において参照動作を行って暗号バンク170内部の適切な暗号器に関係付けられたハント・グループの指定を確認する。次に、ステップ1027において、コントローラ152が、交換機151に信号で合図を送り、一方の当事者(即ち、「暗号化開始信号」を発生しなかった方の当事者)を保留し、かつ選択された暗号器の種類に関係付けられたハント・グループに呼を発するようにさせる。そのハント・グループが呼び出されると、次に利用可能な適切な種類の暗号器(例えば、図1の暗号器172)が交換機151によって選択される。しかしながら、選択された種類の暗号器が利用できない場合(ステップ1029)、処理は終了する(ステップ1009)。

【0058】暗号器172のトレーニング(ステップ1031)は、図5に関連して既に説明した過程と同じ過程をたどるが、これが完了すると、ステップ1033において、トレーニング期間中に他方の当事者(即ち、ス

テップ1023の暗号化要求に関係していない当事者)が通信路の残りの部分で送られるメッセージの暗号化の開始要求を信号で送ったかどうかについて判断を行う。送っていない場合、ステップ1027において保留された呼およびコントローラ152から暗号器172への呼がステップ1035においてブリッジされる。この時点で、交換機151に適切な制御信号を送ることによって通信路からコントローラ152を取り除くことができ、これによって交換機の内部にブリッジ接続が確立される。しかしながら、通信路におけるコントローラ152によって暗号器のトレーニングが完了したのであるから、通信路からコントローラ152を除去することが、CPE101および102ならびに暗号器172および174が暗号化通信を継続する能力を妨げないことが重要である。これについては、コントローラ152により通信路に無視できる程度の遅延および周波数歪しか挿入されないことを保証することによって、対処することができる。

【0059】他方の当事者が暗号開始の要求信号を送った場合、その当事者の暗号器の種類に関してステップ1025~1031が繰り返される。このようにして、安全から安全の呼が完成する。

【0060】図11~15のハードウェア図によって図10に示した処理を説明する。図11は、ステップ1019が完了した後のCPE101および102、交換機151およびコントローラ152の配置を表す。コントローラ152は発呼者と被呼者との間に存在するクリアな通信路に挿入されている点に注目する必要がある。

【0061】図12は、ステップ1031が完了した後の同じハードウェア構成要素の配置を示す。処理のこの点において、暗号器172は、CPE101の中の暗号化モジュールについてトレーニング中であり、同時にCPE102の被呼者は、保留状態にあり、一般に、他方の当事者とトレーニングが進行中であることを示す告知をコントローラ152の音声応答ユニット153から受信している状態である。

【0062】図13において、安全からクリアの呼について図10の処理が完了する。ハードウェアの配置は、通信路にコントローラ152がないことを除けば、図3に示したものと類似している。

【0063】図14は、ステップ1033において他方の当事者が暗号化を開始するときに、安全から安全の呼に伴う付加的な要素を示す。同図において、被呼者のCPE102にある暗号化モジュールは、第2の暗号器、即ち暗号器174についてトレーニング中である。トレーニング処理が終了すると、ハードウェアの配置は、図15に示したようになる。この配置は、コントローラ152が通信路にないことを除けば、図7に示したものと類似したものとなる。

【0064】以上の説明は、本発明の一実施例に関する

もので、この技術分野の当業者であれば、本発明の種々の変形例が考えられるが、それらはいずれも本発明の技術的範囲に含まれる。いくつかの例を示す。

【0065】不正およびその他の悪用を防ぐために、安全ノード150にアクセスするための呼の発呼者あたりの試行回数（ANIを監視することにより判定する）を追跡するように安全ノードを構成してもよい。所定の期間内に所定の回数の試行が行われた後、安全ノードは、その発呼者（ANI）がそれ以上そのノードにアクセスしようとするのを自動的に阻止する。安全な番号指定も提供することができる。これにより、被呼者の番号を入力する前にSTDまたはCPEから安全ノードへの呼の安全が確保されるので、被呼者の番号および（または）発呼者のダイヤル・ボタンが盗聴者に知られることがない。

【0066】本発明は、既に利用可能な種々のサービスのみならず将来提供する予定の新たな多くのサービスとの関連においても使用することができる。例えば、安全な音声およびファクシミリの記憶および検索では、クリアから安全の呼をサポートし、呼び出し時に応答がないか話中の場合の入接続メッセージを安全なメールボックスに渡せるようにすると、そのメッセージは被呼者により後にアクセスできるように暗号化された形式で記憶される。これにより、暗号化されたメッセージが資格のある当事者によって取り出されるまで、そのメッセージを安全な場所に保管することができる。発呼者は、そのメッセージが意図する受信者に届くまで、情報の安全が保証される。

【0067】前記の説明の部分は音声の呼について述べたが、本発明は、あらゆる種類のデータの安全な通信にも関連付けて同様に利用することができる。例えば、本発明は、PC間の通信およびPCとメインフレーム・コンピュータとの間の通信の保護に対しては理想的である。この用途には、電話装置と電話回線との間のSTDインタフェースを適切に変更するだけでよく、これは普通の技術で容易に実現できる。同様に、安全なファクシミリを用いて、ファクシミリ装置間の通信、ならびにファクシミリの記憶および転送サービスを保護することができる。ファクシミリ受信（ファクシミリが誰に配信されたか）の正真性の証明を与えることもできる。

【0068】通話の課金については、種々の解決方法が可能である。例えば、発信側および受信側のANIおよび各利用者のID番号に関係付けられた通話時間の情報を安全ノード150が捕捉するように安全ノードを構成してもよい。この情報を主課金番号と共に課金評価／書式化システム187に渡し、その加入者の発信通話表に基づいて処理して、その加入者の請求額に加える。呼は、発信地と安全ノードと受信地との間ではなく発信地と受信地との間の呼の流れに基づいて評価される。従って、安全ノード150との間の呼のやりとりの費用は、

一般に暗号化／暗号解読の特別料金の一部となり、加入者の請求書に項目としては現れないことになる。課金は、被呼者から安全ノード150に回答指示が与えられた時に開始される。加入者が発信した呼（即ち、安全からクリアの呼、安全から安全の呼）に対しては異なる課金構造を用いることができる。この場合の通話の費用は、発信した加入者の請求額に適用することができる。これに対し、クリアから安全の呼の場合は、（コレクト・コールのように）受信側の加入者が通話費用の責任を負うことになる。

【0069】最後に、以上の説明では交換機151およびコントローラ152を別個の装置として述べたが、呼の監視、音声プロンプトの発生および応答の収集、情報の記憶、蓄積プログラムの制御下での接続、および種々の関係付けられた機能の実行が可能な単一の「インテリジェント交換機」を電気通信網の中に配置して代用することができる。

#### 【0070】

【発明の効果】以上述べたように、本発明によれば、呼の当事者の双方がハンドシェイク・プロトコルおよび暗号アルゴリズムの異なる安全装置を有する場合も、また当事者の一方のみが安全装置を有する場合も、比較的安全な通信を行うことができる。

#### 【図面の簡単な説明】

【図1】本発明によって構成された安全ノードを例示するブロック図である。

【図2】「安全からクリア」の通信経路、即ち発呼者（CPE101）と安全ノードとの間の安全な接続、および安全なノードと被呼者（CPE102）との間のクリアな接続を設定するために図1のコントローラ152において実行されるステップを例示する流れ図である。

【図3】安全からクリアの通信を開始する過程を説明し、そのような呼またはメッセージに対する図1の構成要素の幾つかを通る経路を例示するために役立つハードウェア流れ図である。

【図4】暗号器バンク170およびCPE101および102の暗号器において実行されるハンドシェイク・ステップを例示する流れ図である。

【図5】「安全から安全」の通信を設定するためにコントローラ152において実行されるステップを例示する流れ図である。

【図6】安全から安全の通信を開始するための設定過程に伴う付加的な要素を示す図3と同様の図である。

【図7】図6の構造を用いて安全から安全の通信が確立された後の経路を示す図である。

【図8】図1のCPE101のような典型的な加入者の構内装置の要素を示すブロック図である。

【図9】暗号器バンクの内部の暗号器172および174などの典型的な暗号器の要素を示すブロック図である。



25

【図10】安全なノード150を用いて安全からクリア、クリアから安全、安全から安全の呼を完成させるための代案の過程を示すブロック図である。

【図11】図10の過程における種々のステップの期間中のハードウェア構造を示す図である。

【図12】図10の過程における種々のステップの期間中のハードウェア構造を示す図である。

【図13】図10の過程における種々のステップの期間中のハードウェア構造を示す図である。

【図14】図10の過程における種々のステップの期間中のハードウェア構造を示す図である。

【図15】図10の過程における種々のステップの期間中のハードウェア構造を示す図である。

#### 【符号の説明】

101、102

加入者構内装置 (CPE)

107、112

市内交換機

108、111

市内交換キャリア (LEC) 局

110 相互交換キャリア交換機

26

115 共通チャネル信号 (CCS) 網

116 信号転送点 (STP=signal transfer point)

120 着信ワッツ (InWATS) データベース (IDB)

150 安全ノード

151 交換機 (SWITCH)

152 交換機コントローラ (SWITCH CONTROLLER, CONTROLLERまたはCONT)

153 音声応答ユニット (VRU)

154 データベース (DB)

156 交換通信網

160 トランク

161 線群

170 暗号器バンク

172、174

暗号器/解読器

180 通話カード・データベース

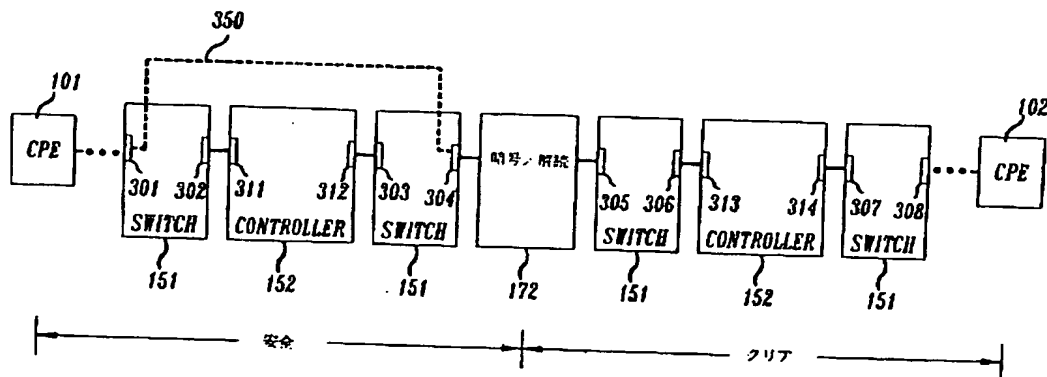
185 記録/課金プロセッサ

187 課金評価/書式化システム

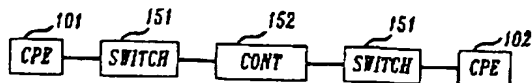
20 191、192

安全電話装置 (STD)

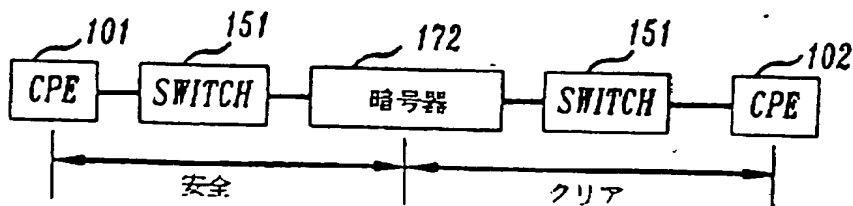
【図3】



【図11】

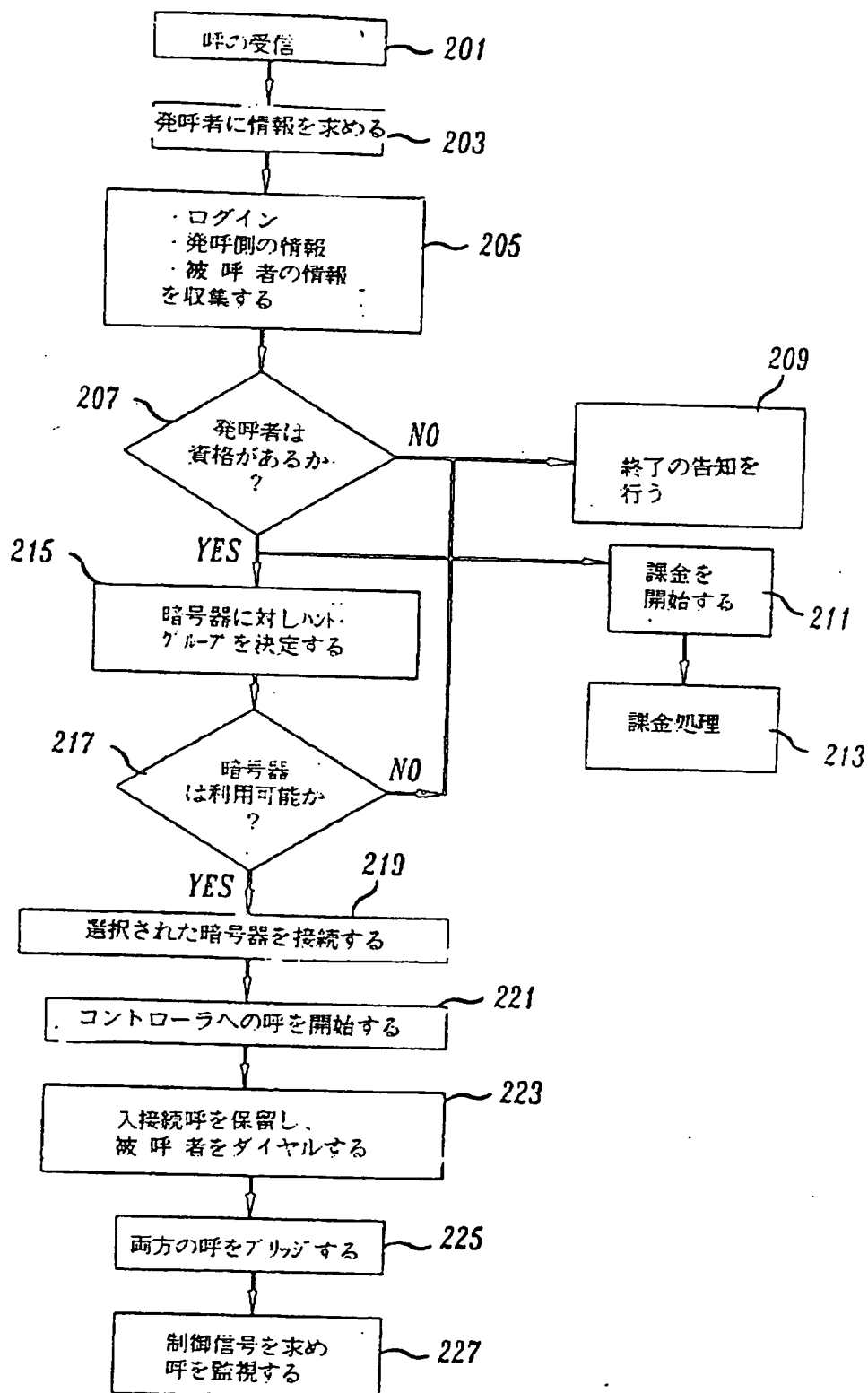


【図13】

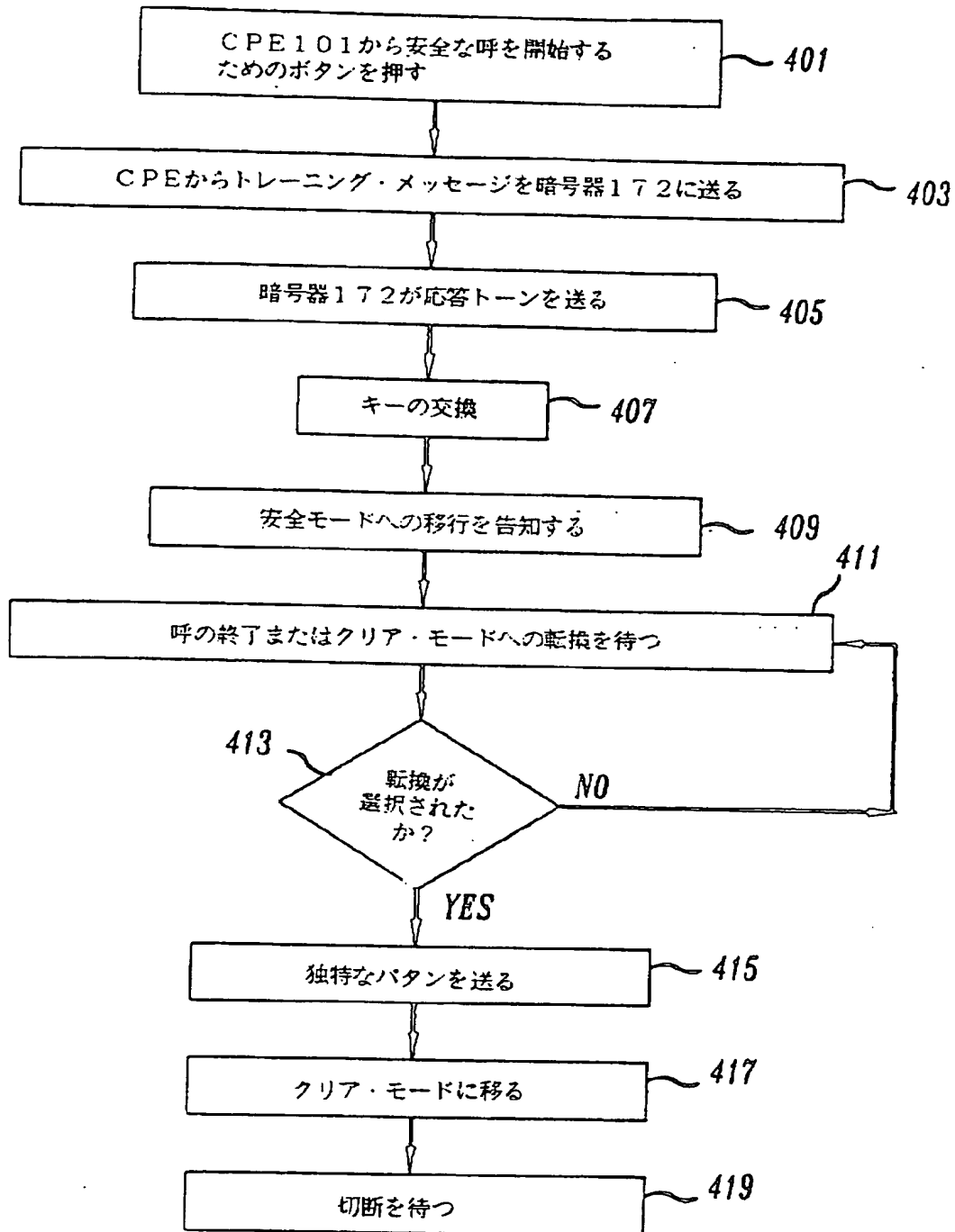




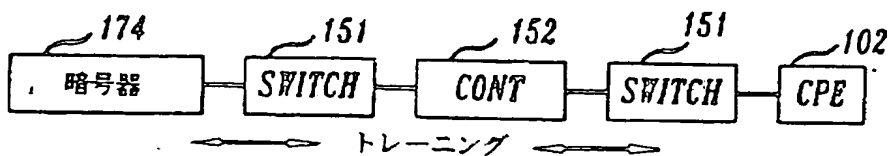
【図2】



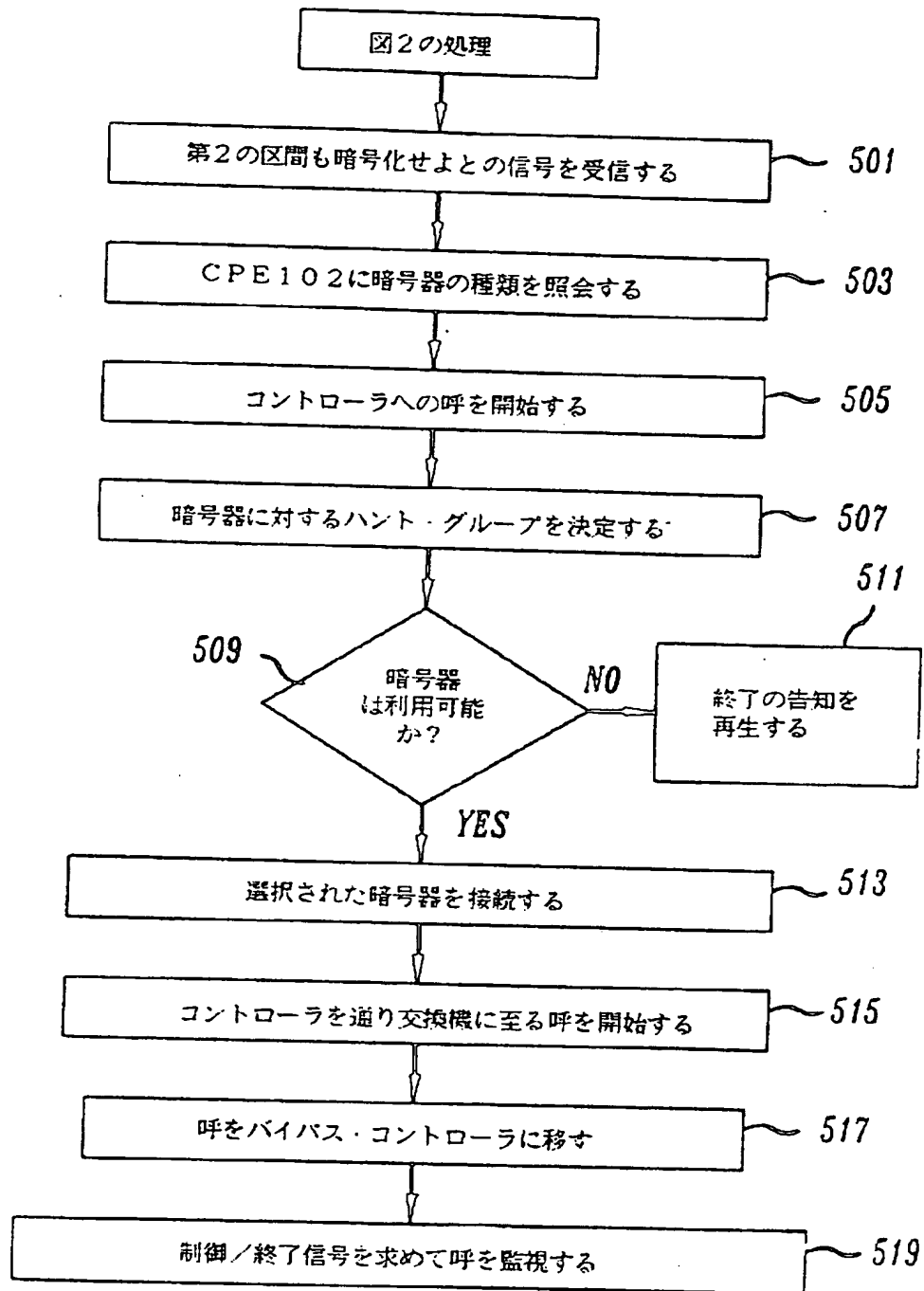
【図4】



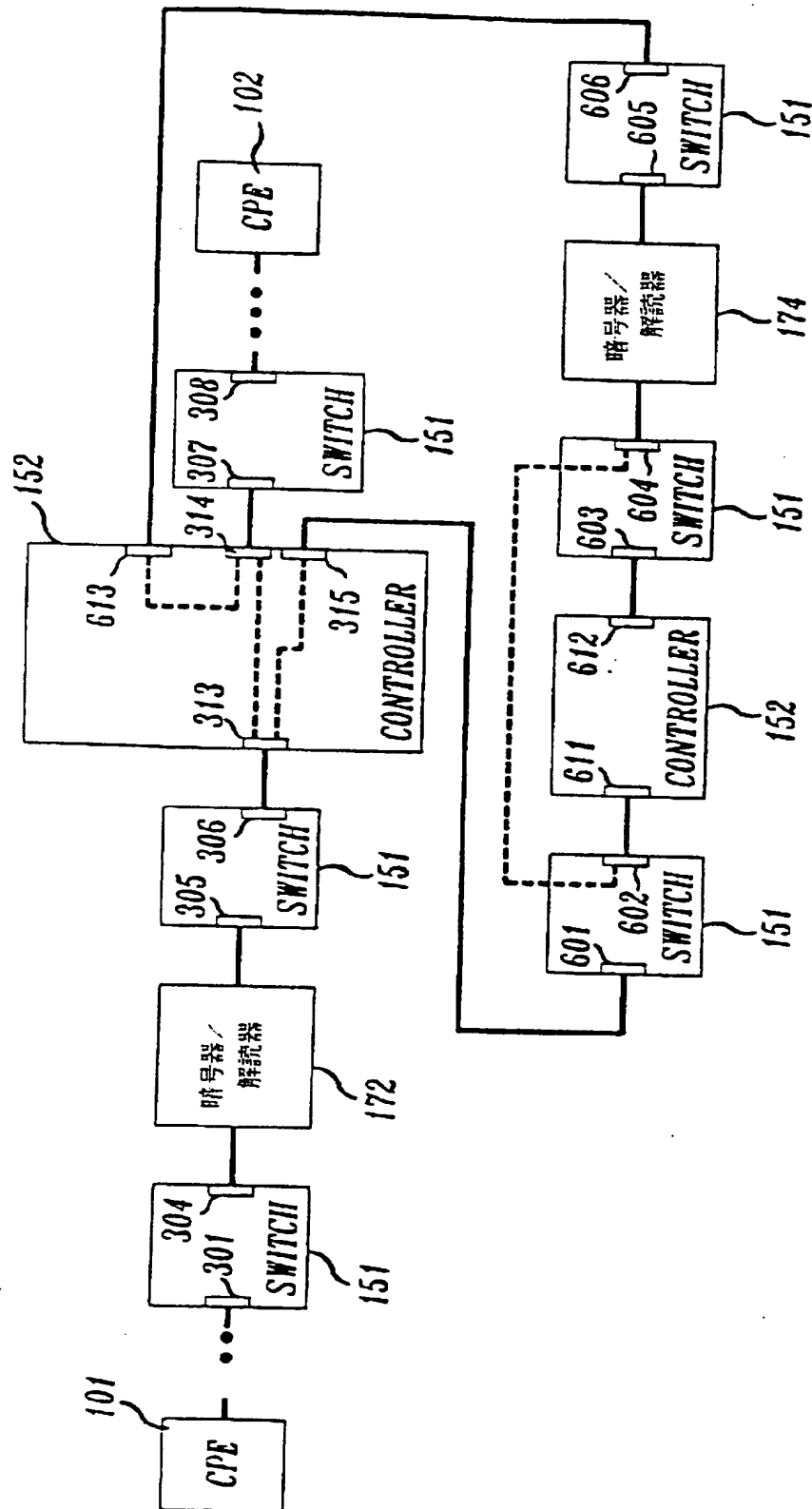
【図14】



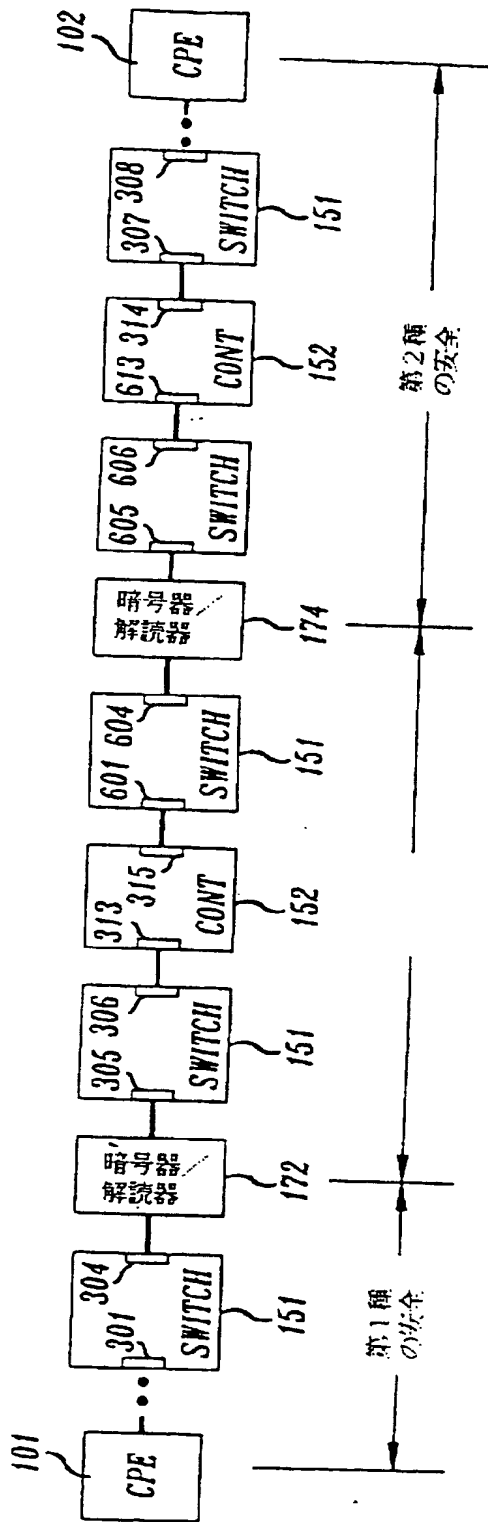
【図5】



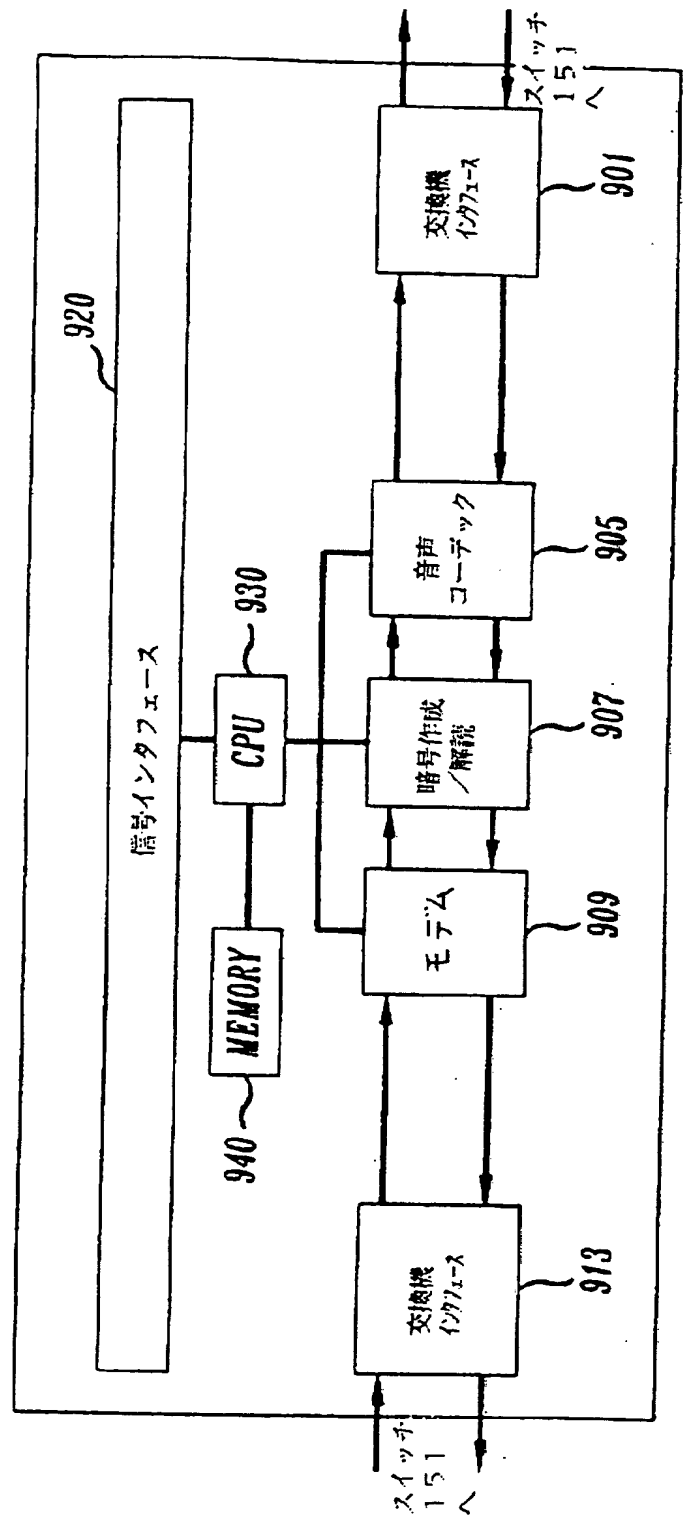
【図6】



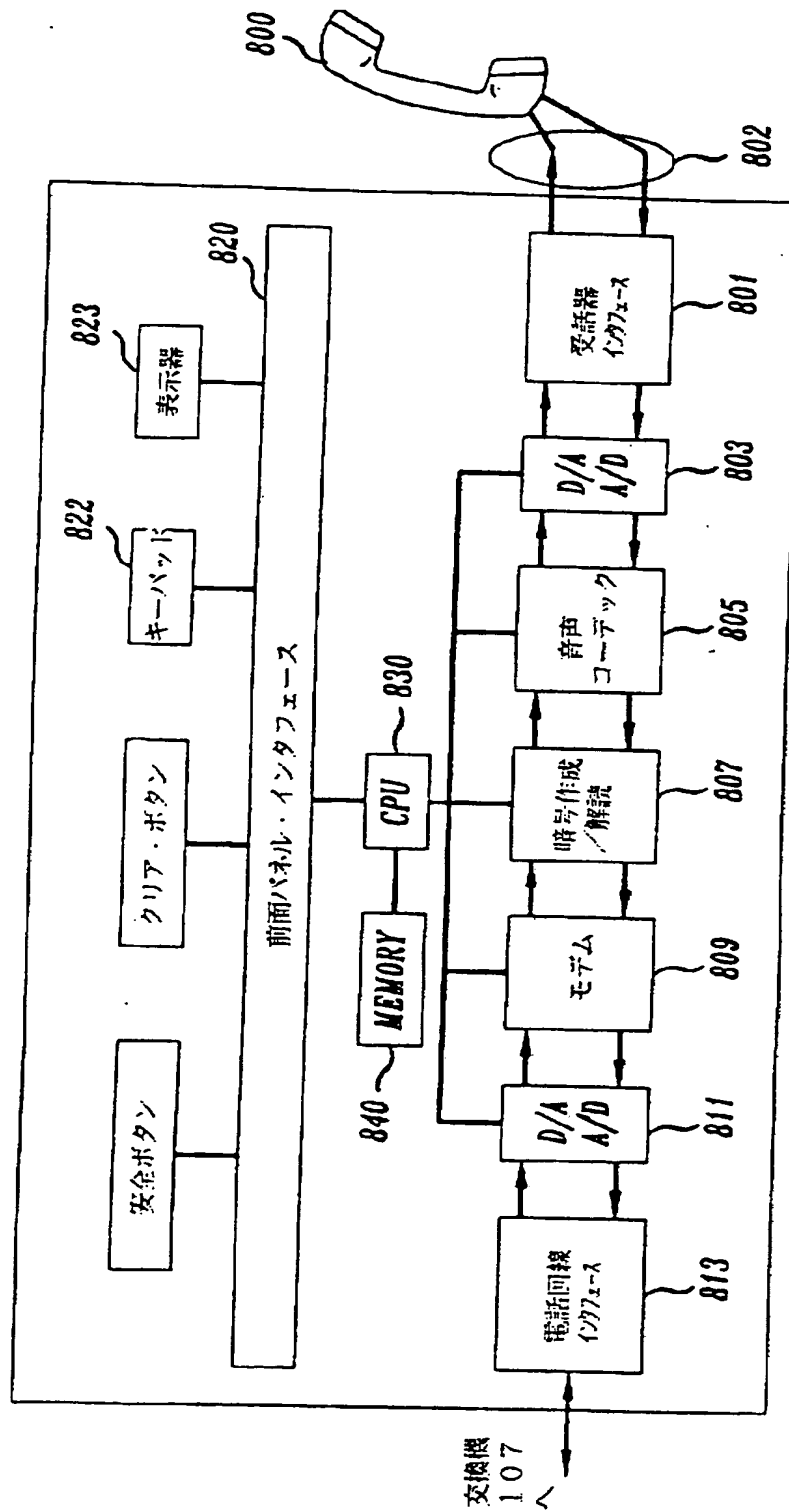
【図7】



【図9】

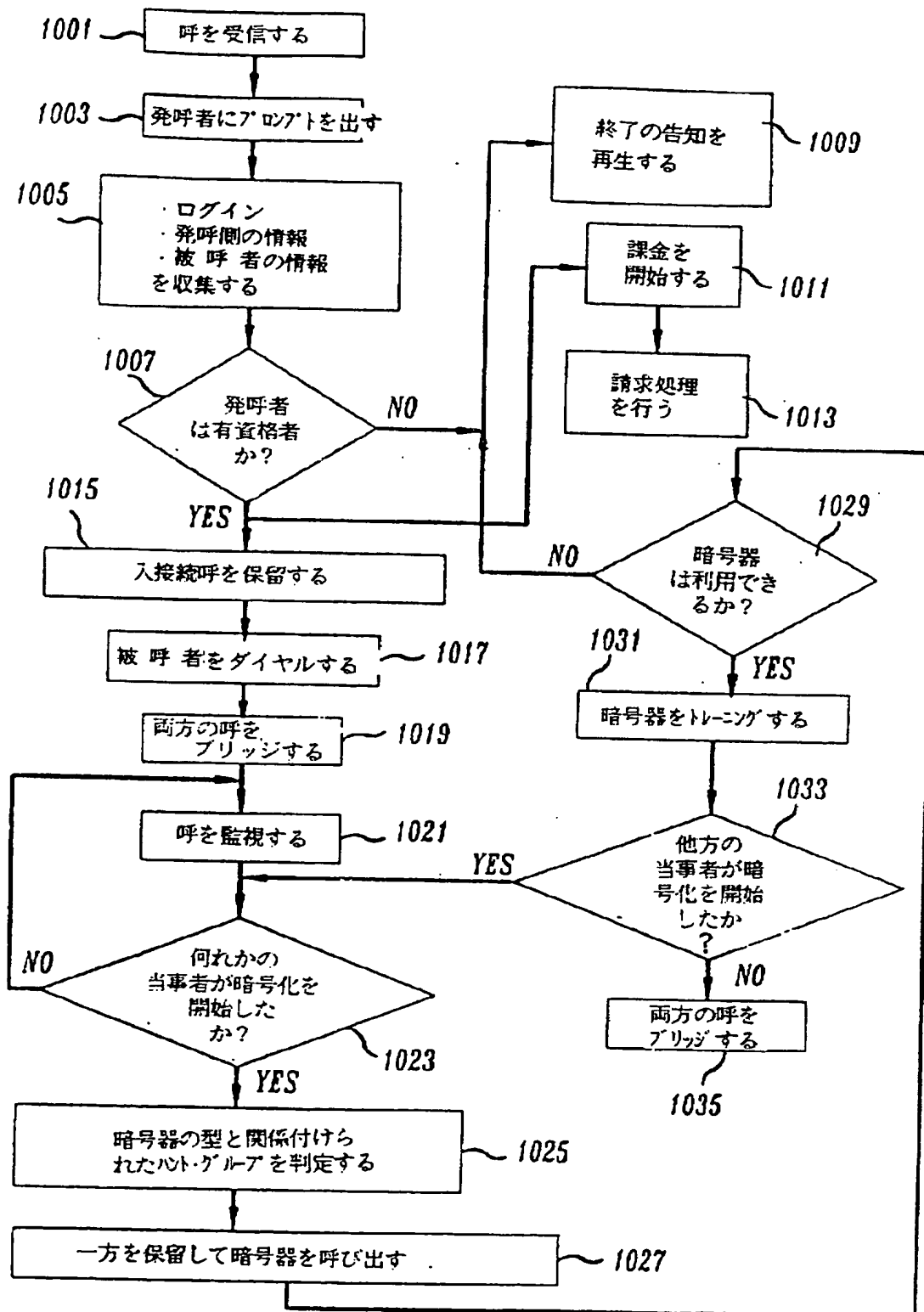


【図8】

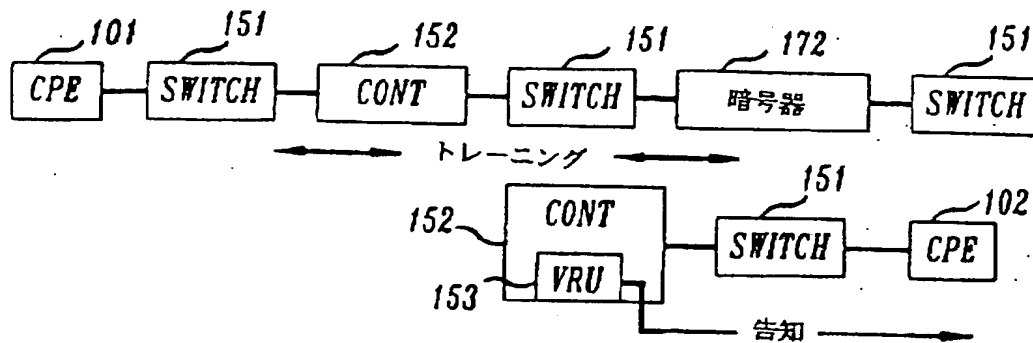




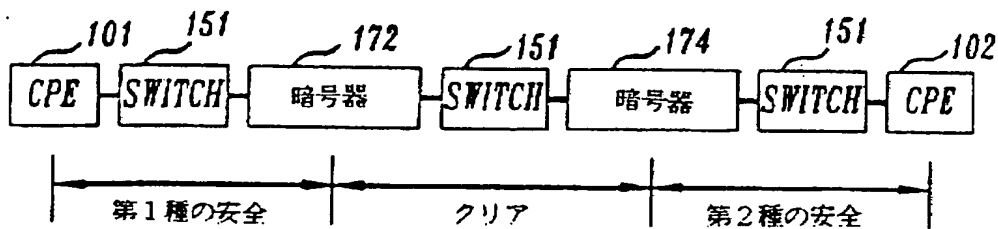
【図10】



【図12】



【図15】



フロントページの続き

(51) Int. Cl. 5

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 12/00

H 0 4 Q 3/545

9076-5K

(72) 発明者 アンドリュー エフ. バルファー  
 アメリカ合衆国 07046 ニュージャージー  
 ー マウンテン レークス、ブルヴァード  
 85

(72) 発明者 マイケル エム. カプラン  
 アメリカ合衆国 01966 マサチューセッ  
 ツ ロックポート、オーシャン アヴェニ  
 ュー 4

(72) 発明者 ブルース イー. マクネア  
 アメリカ合衆国 07733 ニュージャージー  
 ー ホルムデル、アイロン ヒル ドライ  
 ヴ 1

(72) 発明者 キャロル エー. ヴェグルジノ ヴイツ  
 アメリカ合衆国 07733 ニュージャージー  
 ー ホルムデル、タコルサ ドライブ 29